(2022) 34 SAcLJ 352
(Published on e-First 6 June 2022)

THE REASONABLENESS STANDARD OF COMPLIANCE IN THE SINGAPORE PERSONAL DATA PROTECTION ACT

The "reasonableness test" establishes the threshold of compliance and accountability under the Singapore Personal Data Protection Act. This "open-ended" test is flexible enough to take into account and react to changes in the scope and uses of personal data to maintain an equilibrium between the interest of individuals in the protection of their personal information on the one hand and the needs of organisations for access to, and the use of, such data on the other. This article seeks to provide a better understanding of how the test works by comparing it to the objective and function of the fair use doctrine in copyright law, and by evaluating how the test has been used and adapted in different situations, obligations and forms of personal data (particularly in the context of the consent and purpose obligations). The importance of keeping the test independent of the concept of "personal data" will also be considered.

Warren B **CHIK**[1]
LLB (National University of Singapore), LLM (Tulane), LLM (UCL);
Associate Professor of Law, Yong Pung How School of Law,
Singapore Management University;
Deputy Director, Centre for AI and Data Governance.

I. Introduction

1 The approach of the Singapore Personal Data Protection Act 2012[2] ("PDPA") to data protection is a pragmatic one, based on a balance of interest between the right of individuals to the protection of their personal data and the needs of organisations in their transactions

1 This research is supported by the National Research Foundation, Singapore under its Emerging Areas of Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author's and do not reflect the views of the National Research Foundation, Singapore.

2 2020 Rev Ed. This was previously known as Act 26 of 2012 as amended by Act 40 of 2020. The 2020 revised edition of the Personal Data Protection Act came into operation on 31 December 2021 and was amended by the Courts (Civil and Criminal Justice) Reform Act 2021 (Act 25 of 2021), which commenced on 1 April 2022.

with the former.[3] The PDPA underwent its first major overhaul after several years of review and many of the amendments entered into force on 1 February 2021.[4] Although the rules for the protection of personal data and the main obligations remain intact, there is a clear shift towards an accountability model for organisations that collect, use and share personal data as well as a move towards giving greater personal control over personal information belonging to the data subject.

2 Some of the most significant changes relating to compliance were made to the obligation requiring consent for the collection, use and disclosure of personal data by organisations (the "consent obligation"). The broadening of the "deemed consent" concept (in particular, deemed consent by notification), the re-categorisation of the exceptions to the consent obligation in the Schedules to the PDPA and the introduction of the "legitimate interest" exception provide greater flexibility and clarity for organisations, freeing them from the onerous task of always having to seek the permission from individuals that they transact with for access to their personal information. These are in effect exceptions to the obligation to seek real and actual consent, which is the freely given, specific, informed and unambiguous indicator of an individual's permission (*eg*, consisting of a clear statement or affirmative action signifying agreement to the collection, use or sharing of one's personal data). Consent must be solicited by organisations and given by individuals for *each of these acts* (*ie*, collection, use and disclosure) severally, although the manner of doing so may be done collectively in the same way and at the same time, all the while subject to a reasonableness standard or test. This test, which is the linchpin of the personal data protection regime in Singapore, is in fact applicable not just to the consent obligation but to every other duty or obligation placed on organisations subject to the PDPA to comply with their statutory obligations. It is a versatile test and its application is modified to suit the nature of the obligation concerned.

---

3 Personal Data Protection Act 2012 (2020 Rev Ed) s 3. There is overarching public interest in achieving this balance between essentially private parties (individuals and natural persons or legal entities), which is to achieve utilitarian goals in the management of personal information (for the greater socio-economic benefit of the country generally). "Public interest" is also explicitly addressed in some of the exceptions to consent: (a) under the First Schedule and Second Schedule (Pts 2 and 3, Div 1); (b) under the First Schedule, Pt 2(2) ("national interest"); (c) and where "public benefit" is a factor in the research purpose analysis (Pt 2, Div 3 and Pt 3, Div 2). Public interest is also implicitly taken into consideration in other exceptions like the First Schedule, Pt 2 ("matters affecting public"), and exceptions to access or correction requirements (under the Fifth and Sixth Schedules) that may impede efficient state or public agency functions or that may inadvertently affect confidentiality interests (national or private).

4 Specifically, ss 2–13, 15–23, 25–38, 40, 41, 43 and 46 of the Personal Data Protection Act 2012 (2020 Rev Ed).

3 Part II of this article will compare how the "reasonableness text" is used in the PDPA directly through the general rule of compliance with the consent obligation as well as indirectly through the exceptions contained in the re-modelled Schedules to the Act. This Part will analyse each of the factors that are to be taken into consideration by organisations, in their independent assessment and data governance processes, and by the Personal Data Protection Commission ("PDPC"), when investigating alleged non-compliance and in updating and drawing up its advisory and sector specific guidelines.

4 The PDPC's administrative decisions have also provided a rich resource on the scope and meaning of "reasonableness" in relation to the purpose of collection and disclosure, and especially in relation to the use, of personal data. Supplementary tests have been developed to determine reasonableness in different situations.

5 Part III will examine the "reasonableness text" and its many forms and permutations, mainly in the context of the purpose limitation obligation. Who the "reasonable person" is, and the appropriateness of his actions in specific circumstances and transactions in relation to another's personal data, will be considered. It will be shown that the "reasonableness assessment" itself is multifaceted and can be adjusted to suit the relevant parties and the nature and context of their interaction.

6 In Part IV, this article will show how the purpose of the "reasonableness test" and its function is similar to how the "fair use" exception had evolved in the Singapore Copyright Act 2021[5] ("SCA"), especially with the shift in both substance and form to the "open-ended" "fair use" doctrine in the US, the concomitant development in the statutory exceptions in the PDPA (similarly based, explicitly or implicitly, on a reasonableness assessment) in relation to the former, and the evolution of the list of explicit acts (*ie*, the nature of the "dealing" or "use") that do not constitute copyright infringement in relation to the latter.

7 Finally, Part V of this article will highlight how the Singapore model and approach compares favourably to that of other countries. This is because the reasonableness standard of compliance and accountability is clear, comprehensive, pragmatic and suitable to its socio-economic context, and because it does not conflate and confuse the standard of statutory compliance with the scope and definition of "personal data" (which should remain "value-neutral") as some other data protection models do.

5 Act 22 of 2021.

8 The overall objective of this article is to highlight the importance of the "reasonableness test" to the functioning of the PDPA, acquaint the reader with the compliance and accountability standard in the PDPA and explain the flexibility of approach in assessing when the standard is breached (with a particular focus on the consent obligation for the collection, use and disclosure of personal data due to significant developments in this area).

II. The obligation to seek consent: Statutory exceptions, factors and considerations

9 The PDPA contains statutory exceptions to the general rule requiring consent. Generally, actual consent is required under the Act.[6] The alternatives to it are the reliance on "deemed consent" and where no consent is required or authorised under any written law, including the PDPA itself.[7] First, actual consent means real consent given without subterfuge such as through false or misleading information or deceptive or misleading practices to elicit permission.[8] Second, it must be informed consent in that the assent must relate to one or more specific and defined purposes or objectives that are notified to the individual concerned.[9] Third, it should be unambiguous, preferably through affirmative action signifying assent although it may be reasonable, in certain cases, to infer or imply consent through the circumstances and/or the conduct of the individual.[10] In relation to the latter (and to "deemed consent"), the Singapore standard is lower than that set in the European Union's

6 Personal Data Protection Act 2012 (2020 Rev Ed) s 13(*a*). See also Art 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR").

7 Personal Data Protection Act 2012 (2020 Rev Ed) s 13(*b*) read with s 17, with reference to the First and Second Schedules.

8 Personal Data Protection Act 2012 (2020 Rev Ed) s 14(2)(*b*).

9 Personal Data Protection Act 2012 (2020 Rev Ed) s 20(1) read with ss 14(1)(*a*) and 18(*b*).

10 See *German European School Singapore* [2019] SGPDPC 8 at [12]–[13], where consent can also be implied from the circumstances or the conduct of the individual in question. In this case, the continued enrolment of a student in the school for a substantial period was taken to constitute acquiescence to the school's bye-laws, including the collection of his personal information (*ie*, hair samples for drug testing) that was in dispute: see *German European School Singapore* [2019] SGPDPC 8 at [24]–[26]. Unlike deemed consent, which can be said to be *a legally recognised* assent, implied consent is a form of actual consent or *permission in fact*.

General Data Protection Regulations[11] ("GDPR"), which requires direct and active action and eschews passivity as a form of assent.[12]

10 Unlike the GDPR, the PDPA also allows for a gradation of legal and legitimate alternatives to real or factual consent besides the statutory exceptions.[13] This includes deemed consent (by an individual voluntarily furnishing personal data to an organisation for a purpose and that it is reasonable to do so),[14] for contractual necessity,[15] and deemed consent by notification provided that it is determined through an assessment that there is no likely adverse impact on the individual who is given a reasonable opportunity to object.[16]

11 It should be noted at the outset that *even where* deemed consent and the statutory exceptions are inapplicable and where actual consent is normally required, there can nevertheless still be circumstances wherein it is appropriate *to not* seek consent. This was made clear in the Personal Data Protection Commissioner's decision in *Jump Rope (Singapore)*.[17] That decision involved the disclosure of the complainant's personal data, including his name and identity number, via electronic mails to various recipient schools by the respondent that was in the business of providing enrichment and sports coaching services (including rope skipping) to schools. The electronic mails were to inform the recipient schools that the complainant was blacklisted as an unsuitable candidate for instruction and coaching, and served as advice not to engage him "to avoid the teaching of wrong values" to their students. On the issue

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (accessed 7 February 2022).

12 Article 4(11) of the GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". See also Article 7 of the GDPR on the conditions for consent.

13 These include the general exceptions under s 4 of the Personal Data Protection Act 2012 (2020 Rev Ed), which includes legal obligations under any other law which shall prevail to the extent that they are inconsistent with the Personal Data Protection Act 2012 (2020 Rev Ed) (s 4(6), that reflects Art 6(1)(c) of the GDPR); and the exceptions to the consent, access and correction requirements under the First to Second (read with s 17), Fifth and Sixth Schedules to the Personal Data Protection Act 2012 (2020 Rev Ed) respectively.

14 Personal Data Protection Act 2012 (2020 Rev Ed) ss 15(1)–15(2).

15 Personal Data Protection Act 2012 (2020 Rev Ed) ss 15(3)–15(10). See also Art 6(1)(b) of the GDPR.

16 Personal Data Protection Act 2012 (2020 Rev Ed) s 15A.

17 *Jump Rope (Singapore)* [2016] SGPDPC 21.

of lack of consent, the Commissioner found that the respondent failed to comply with the PDPC.[18] However, he also clarified that there may be circumstances where it may be considered appropriate by a reasonable person for consent not to be sought:[19]

> … In a suitable case, there can be valid business or legal reasons for the blacklisting to be disclosed in order to warn the Respondent's clients, notwithstanding that it may contain some personal data about the Complainant. It may not be desirable to expect organisations to obtain consent from the person(s) that is the subject of the disciplinary action, dismissal and blacklisting, as consent is unlikely to be forthcoming in all cases. …
>
> In a suitable case, disclosure of personal data that is relevant to the matter, by an organisation without consent nor notification, may be made if it is reasonable to do so. This is because the standard of 'reasonableness' underpins the PDPA, as specifically provided for under Section 11(1) of the PDPA. Section 11(1) of the PDPA provides that '*[i]n meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances*'. In this regard, an organisation can inform its clients that Person A (name and former designation) has left its employment on a specific date. Further, the Commission considers that it is conceivable that there can be circumstances where an organisation may be acting reasonably in disclosing personal data in respect of a blacklisting to warn others, without consent, and apart from the scheduled exceptions; but these are limited, and very much depends on the context and circumstances in which the disclosure was made. For example, if there was credible evidence of fraudulent conduct that a former member of staff is misrepresenting his status of employment and association with his former employer, it may be reasonable for the former employer to write to existing customers informing them of the facts. …

12 This is where the PDPA majorly departs from a "closed list" system whereby consent can only be dispensed with in relation to specific forms of use or processing and under specified conditions.[20] In other words,

---

18 *Jump Rope (Singapore)* [2016] SGPDPC 21 at [12]. There was no legal justification for not seeking consent as the respondent went beyond what was reasonable or appropriate.

19 *Jump Rope (Singapore)* [2016] SGPDPC 21 at [10]–[11]. It may be noted that "business and legal reasons" was under consideration as a new statutory exception to be included in the 2021 amendments but was replaced by the broader "legitimate interests" exception.

20 See *eg*, Art 6 of the GDPR which provides for the lawful processing of personal data only on give general bases besides consent for one or more specific purposes. These include processing necessary for: (a) contractual performance; (b) compliance with a legal obligation; (c) to protect the vital interests of the data subject or another natural person; (d) the performance of a task carried out in the public interest or in exercise of official authority vested in the data controller; and (e) for a legitimate interest that overrides the interests of the individual. These other purposes currently exist as statutory exceptions in the Personal Data Protection Act 2012, which shall be elucidated later in this article.

(cont'd on the next page)

there are unspecified circumstances where consent is not required and these circumstances are non-exhaustive and can change and evolve over time. Although these comments were made in relation to the disclosure of personal data, there may be situations where the collection or use of personal data without permission can also be considered appropriate to the reasonable person. The context also matters and as the socio-cultural norms and expectations (which form part of the "circumstances") can change over time, so too what can be considered appropriate to the reasonable "objective" person.[21]

13 This flexibility accorded by the general and residual "reasonableness" compliance standard is supplemented by exceptions, such as the "legitimate interests" exception. The general compliance standard can react to situations where it is impracticable to obtain consent for purposes that may not have been foreseen or anticipated in advance. On the other hand, the statutory exceptions and the guidance provided by mandatory assessment exercises (or factors for consideration) help to reduce the uncertainties of the general concept of "reasonableness".

14 Aside from this, the statutory exceptions are consistent with international norms, which is even more apparent after the "re-structuring" and updating exercise by the Personal Data Protection (Amendment) Act.[22] It is also noteworthy that some of the factors and considerations that emerged from the "jurisprudence" of the PDPC administrative decisions are incorporated into the Act in the recent amendments.[23] Hence, the exceptions, together with the albeit non-legally binding examples from the PDPC's guidelines and other materials,[24] can be viewed as explicit examples or scenarios where it would be reasonable not to have to seek permission or obtain consent in relation to the personal data in question.

---

21 See *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 9.5 wherein it is stated that the standard is "evolutionary".

22 Act 40 of 2020.

23 See *Jump Rope (Singapore)* [2016] SGPDPC 21 at [10] on the "valid business or legal reasons" basis, which was earlier proposed as an exception but that can now come under the scope of the "legitimate interests" exception.

24 Personal Data Protection Act 2012 (2020 Rev Ed) s 18. See, *eg*, *Public Consultation Paper: Draft Personal Data Protection (Amendment) Bill, Including Related Amendments to the Spam Control Act* (Ministry of Communications and Information & The Personal Data Protection Commission, 14 May 2020) at paras 40–42 and *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at paras 12.21–12.23 (deemed consent), 12.63 (legitimate interests), 12.77 (business improvement) and 12.86 (publicly available data, where there are illustrations of "reasonable expectation" of personal data collection (or otherwise) in a public space are given at paras 12.90 and 12.94).

15 These also relate only to eschewing consent for collection, use or disclosure of personal data and does not mean that the other obligations of notification and purpose limitation need not be complied with.[25] In fact, there may be greater reason to more strictly require and enforce these obligations to counterweigh the lack of actual consent. In some cases, for example, notification may be a factor in the reasonableness assessment relating to lack of actual consent. In fact, this is precisely how the new "deemed consent by notification" provision works.[26] Moreover, the notification obligation and the purpose limitation obligation must also independently meet the reasonableness criteria. For example, a debt collecting agency obtaining consent by a borrower, at the time when the loan was made, to be filmed by the agency during debt collection in the event of a default or a delay in payment for the purpose of posting the recording on social media for public shaming is unlikely to be considered by a reasonable person to be appropriate.[27]

16 The exceptions to consent can generally be categorised into those that fall within public or national interest and that which come under business interests. In relation to the latter, a balance of interest assessment is often required, consistent with the objective of the PDPR, whereas it is not required for the former, which is consistent with the PDPR approach to exempt public agencies from the Act (although "matters affecting public" has a broader scope that just matters relating to the work of the authorities).

---

25 See *Jump Rope (Singapore)* [2016] SGPDPC 21 at [10] where the Commissioner stated that even where it is reasonable not to seek consent, "organisation[s] should still comply with the neighbouring obligations of consent, namely, the notification obligation and the purpose limitation obligation … [by only disclosing] what a reasonable person would consider appropriate in the circumstances, and notifying the [individual concerned] about the disclosure to be made".

26 Personal Data Protection Act 2012 (2020 Rev Ed) s 15A.

27 *Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7 at [7]. In such a scenario, the consent itself could be vitiated as having been obtained through unfair, deceptive or misleading practices. See also Sections 14(2) and 14(3) of the Personal Data Protection Act 2012 (2020 Rev Ed) and *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 13(c). On the other hand, if the purpose was for the agency to ensure that the debt collector was acting in a responsible and lawful manner only, then it would more likely be reasonable and appropriate to record the transaction: *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 8. In comparison, a school providing educational services collecting personal data to perform drug testing is reasonable and the means of doing so through the collection of hair samples can be considered a "reasonably appropriate means" to achieve that aim. See *German European School Singapore* [2019] SGPDPC 8, where the Commissioner dealt with what is "reasonable" and "appropriate" holistically.

Objective	Section 17 of the PDPA	Article 6 of the GDPR
Commercial requirement	[Section 15 on deemed consent generally and under s 15(6) relating to what is reasonably necessary for the performance or conclusion of a contract]	Necessary in preparation to enter into or for the performance of a contract.[28]
Individual's interest	Vital interests of individuals:[29] (a) Necessary for an individual's interests and (i) consent cannot be obtained in a timely way; or (ii) the individual would not reasonably be expected to withhold consent.[30] (b) Necessary to respond to an emergency that threatens the life, health or safety of the individual or another.[31] (c) Necessary for an individual's interests and (i) consent cannot be obtained in a timely way; and (ii) there are reasonable grounds to believe that the health or safety of the individual or another will be seriously affected.[32] (d) To contact the next-of-kin or a friend if any injured, ill or deceased individual.[33]	Necessary to protect the vital interests of the individual or another natural person.[34]

28 GDPR Art 6(1)(b).
29 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 1.
30 *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 1(1). The individual concerned must be notified as soon as practicable (see para 1(2)).
31 *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 2.
32 *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 3.
33 *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 4.
34 GDPR Art 6(1)(d).

Objective	Section 17 of the PDPA	Article 6 of the GDPR
National interest	Matters affecting public:[35] (a) National Interest. (b) Publicly Available. (c) Solely for artistic or literary purposes. (d) Solely for historical purposes if a reasonable person would not consider it too sensitive at that time. (e) By a news organisation solely for its news activity.	Necessary for national interest (or the exercise of "official authority")[36] that "shall meet an objective of public interest and be proportionate to the legitimate aim pursued".[37]
Private interests	Legitimate interests:[38] (a) Wherein the legitimate interests of the organisation or another person should outweigh any adverse effect on the individual and comply with other requirements including notification of the individual and reducing probable adverse effects. (b) Necessary for evaluative purposes. (c) Necessary for investigation or proceedings. (d) Necessary for debt recovery or payment. (e) Necessary for the provision of, or to obtain, legal services. (f) By a credit bureau, for the purpose of preparing or in relation to providing a credit report. (g) To confer or administer an interest or benefit under a private trust or benefit plan. (h) To provide a service for the personal or domestic purposes of the individual.	Necessary for "legitimate interests" of the data controller or a third party, except where overridden by the interests or fundamental rights and freedoms of the data subject.[39]

35 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 2.
36 GDPR Art 6(1)(e).
37 GDPR Art 6(3).
38 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 3.
39 GDPR Art 6(1)(f). For Arts 6(3)(b)–(f), factors such as the link in purposes for collection and use, the context of collection, the relationship of the parties, the

(cont'd on the next page)

Objective	Section 17 of the PDPA	Article 6 of the GDPR
	(i) For the purposes of managing or terminating employment or appointment, and in relation to a business or profession. (j) Business asset transactions.[40] (k) Business improvement purposes.[41] (l) Research purposes (used or disclosed for research) that cannot reasonably be accomplished except in individually identifiable form, there is clear public benefit, the result will not be used to make any decisions that affects the individual, if published it will not identify the individual, and (in relation to disclosure only) it is impracticable to seek consent.[42]	

Others	Section 13 of the PDPA	GDPR
Legal obligations (and legally sanctioned exemption)	(a) where the individual is deemed to have given consent;[43] or (b) the collection, use or disclosure is required or authorised under any written law.[44]	Necessary to comply with legal obligations.[45]

nature of the data, the possible consequences (*ie*, impact) on the individual and the existence of appropriate safeguards must be taken into account.

40 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 4.

41 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 5 and Second Schedule, Pt 2, Div 2.

42 Personal Data Protection Act 2012 (2020 Rev Ed) Second Schedule, Pt 2, Div 3 and Pt 3, Div 2.

43 Personal Data Protection Act 2012 (2020 Rev Ed) s 13(*a*).

44 Personal Data Protection Act 2012 (2020 Rev Ed) s 13(*b*).

45 GDPR Art 6(1)(c).

Others	PDPA	Article 23 of the GDPR
National or public interest	Collection and use disclosed *by* a public agency and consistent with the purpose of disclosure;[46] or disclosure *to* a public agency that is necessary in the public interest.[47]	Restrictions relating to national interest and the performance of governmental functions that "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society".[48]

Table 1: Listed exceptions to the consent requirement under the Personal Data Protection Act 2012 and the General Data Protection Regulations

17 It is noteworthy that even within the GDPR "closed list" exemption categories, an assessment must be made of relevant factors to determine whether the processing or use for another (or further) purpose is compatible with that which the personal data was collected in the first place. This is not dissimilar to how the "deemed consent" provisions operate in the Singapore PDPA and provide the justification for the exceptions to the data subject's consent (and the GDPR Art 23 restrictions, which bear its own form of assessment). As such, there is a measure of "reasonableness-type" evaluation even within this narrower approach or category of exceptions.

18 This potential for expansion of legal bases for processing beyond consent within the other categories of lawful processing is most apparent on the legitimate interests basis wherein the interests for usage concerned can encompass those that were not present at the point in time when the personal data was collected. On the other hand, it should be noted that the emphasis on "necessity", rather than "reasonableness", is indicative of a stricter standard for any deviation from the default rule to seek consent (not just on the basis of the layman's interpretation of these terms as "essential" and "fair" respectively). This deduction is

46 Personal Data Protection Act 2012 (2020 Rev Ed) Second Schedule, Pt 1 and Pt 2, Div 1.

47 Personal Data Protection Act 2012 (2020 Rev Ed) Second Schedule, Pt 3, Div 1.

48 GDPR Art 23(1). Considerations such as the purposes of processing, type of personal data, scope of restriction, risks to rights and freedoms of the individual concerned, *etc*, have to be considered where relevant (GDPR Art 23(2)).

based on the difference in the foundation of the data protection regime between the Singapore PDPA and the EU's GDPR; with the former focused on balancing competing interests, while the latter is premised on the fundamental right to privacy. This is also explicit in the "legitimate interest" exception itself in the GDPR which states that the exception must not only be "necessary" but it can be "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".[49]

III. The purpose limitation and consent obligations: The "reasonableness text" and its variants

19 The underlying test to determine whether the threshold of obligations under the PDPA is breached is based on whether the data collector or "organisation" acted "reasonably"; that is, in a manner that will be objectively determined to be "appropriate in the circumstances" by a "reasonable person".[50] This "reasonableness test" appears in both the purpose provision and the general compliance provisions of the Act.[51] It also appears throughout the Act in relation to various obligations, but is contextualised and purpose-fitted to the nature of the obligation in question.[52] The "appropriateness" relates more specifically to the objective of the organisation in what it does with a person's data. Hence it provides the subjective context within which reasonableness of behaviour is to be assessed.

20 Thus, reasonableness can apply to the general standard of conduct when it comes to the management of personal information, which includes the role of the data protection officer whose responsibility

49 GDPR Art 6(1)(f). Article 1(2) of the GDPR also states that the objective of the Regulations is to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of their personal data.

50 See *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 9.

51 Personal Data Protection Act 2012 (2020 Rev Ed) ss 3 and 11(1).

52 *Ie*, the "reasonableness text" and how it applies may differ in relation to the obligation to seek consent (or otherwise), of giving notice and in relation to the purpose of personal data collection, use or disclosure as the case may be. In some cases, the reasonableness of an act or objective may have an impact on the assessment of reasonableness in compliance in relation to another obligation. For example, the giving of notification and the nature, type or purpose of personal data can be a factor or a reason to justify not seeking the consent of the individual. In some cases, it may even be reasonable not to seek consent *and* notify the data subject, although the purpose limitation obligation remains to delimit the functions to which the personal data may be put to use. What is reasonable may be unfettered or may require adherence to certain other conditions.

is to ensure his or her organisation's compliance with the Act. It is also consistent with the organisation's obligation of accountability (including the data intermediary) for personal data in its possession or control.[53] In relation to specific obligations, it must be noted that the reasonableness standard applies to each obligation separately (*eg*, even with express consent, a purpose for use may not be reasonable; and *vice versa*, even in the absence of consent, the purpose of use may be reasonable). In relation to the other obligations referenced in the previous paragraph, the notable ones that the reasonableness standard is often applied is the protection obligation that must be met by "reasonable security arrangements" – including technical or administrative measures – to prevent breach or leak of personal data. Other than some complaints relating to the consent and purpose limitation obligations, statistically, the most complaints relate to the lack of compliance with the security obligation.

21 As such, there is a singular test running throughout all the obligations of the Act, and the terms "reasonable" or "appropriate" may be used interchangeably and have indeed been so used even in the Commissioner's decisions.[54] However, it is more accurate, and also advisable (to avoid doubt or misunderstanding), to use the entire phrase "appropriate to the reasonable person under the circumstances" for a more accurate description of the assessment exercise. However, for the purpose of brevity, it shall be referred to as the "reasonableness test" in this article.

22 In order to determine what is "reasonable", other measures may be useful depending on the nature of the personal information (*eg*, whether sensitive or not), the relationship between the organisation and the data subject or "individual", and the purpose of the collection, use or disclosure (severally or combined) in a specific case. The "reasonable person" is an objective third party, although when assessing appropriateness, that person may take into account the perspectives of the parties concerned, as will be apparent from the factors that may be used in assessing "reasonableness", which will be explained next. In any case, for the organisation that has to comply with the statutory requirements, it is especially advisable to consider it from the individual's perspective and expectations.

23 The considerations in the following paragraphs, which are not mutually exclusive, can be useful in assessing reasonableness. The tests of necessity and proportionality – which may be appropriately used in

53 Personal Data Protection Act 2012 (2020 Rev Ed) s 13(*b*).

54 Described interchangeably as "appropriate or reasonable step" in *Jump Rope (Singapore)* [2016] SGPDPC 21 at [12].

relation to the organisation's purpose for, and the nature of, the personal data as well as the objective of the obligation concerned – appears in various provisions of the Act and have been utilised in PDPC decisions. The tests for "legitimate interest" (of the data controller organisation) or individual's vital interest (*vis-à-vis* the private sector organisation), integral business-related transactions and exceptions on matters affecting the public, and how they relate to the reasonableness criteria (and *vice versa*), will also be explained. It should be noted that most of these cases relate to the purpose limitation obligation.

A. Necessity

24 Where personal data is taken, utilised or shared for what is considered a necessary purpose, which may also be based on public interest grounds, it can strengthen an organisation's justification that its actions meet the reasonableness threshold.

25 The necessity test is also appropriate for the handling of certain types of information, such as sensitive data, and/or the management of personal data in certain situations like for national emergency such as the need for contact tracing and the detection, isolation and treatment of people with COVID-19.

26 In *Re Naturally Plus Singapore Pte Limited*,[55] the PDPC held that the organisation did not breach the purpose limitation obligation in collecting photocopies of the front of individuals' credit cards and identification cards or work permits, for the purpose of identity verification and authentication, and that alternative forms of identification would not have been adequate in the context of the situation. On the other hand, if *alternatives* were adequate and the sensitive data was not necessary, then the organisation would have breached its obligations.[56]

27 Necessity has also been explicitly "built into" the Act in the form of certain types of exclusions. It appears in the deemed consent provision as well as in exclusions from consent for certain types of collection, use and disclosure. The characteristics of necessity, for example, appear directly such as in relation to data collection, use or disclosure: For the vital interests of individuals or in response to an emergency that threatens

55 [2017] PDP Digest 230.

56 In relation to the collection, use or disclosure of a photocopy of a person's identification card or number, the *Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers* (Personal Data Protection Commission, 31 August 2018) also states that the act must be necessary for the purpose of accurate verification of the identity of the individual: see para 5.1.

life, health or safety of a natural person, for evaluative purposes, and for police investigations, debt payment or collection, or legal services and proceedings.[57]

28 In *Re My Digital Lock Pte Ltd*,[58] the PDPC in considering the necessity for investigations and proceedings and the provision of legal services exceptions in relation to the disclosure of personal data, noted that the disclosure would not be considered necessary for the organisation's objectives if there were *other ways* of achieving them.

29 There is an important distinction to be made here between "necessity" as a more "appropriate" *alternative* to "reasonableness" as a test, and "necessity" as a *factor* to determine reasonableness. First, the "necessity" factor is an alternative to the reasonableness criteria and is used where it is more well suited to the situation or to the purpose. In other words, it is synonymous to reasonableness, and is used in circumstances where it is more appropriate and useful.[59] Second, "necessity" is also sometimes weighted against another factor to justify an exception to consent; in other words, to determine what is reasonable. In the latter case, it is used as a factor to determine reasonableness and to legitimise the exception, especially in situations where the objective is vague (*eg*, requiring subjective judgment) and must be further narrowed in order to meet the general compliance threshold. For example, the PDPC has in its guidelines suggested that data analytics can fall within the purpose of providing a product or service so as to be reasonably included in the consent from an individual.[60]

30 In some cases, it is explicit; in others, the necessity (or practicability and proportionality, for that matter) assessments are inherent in an exception. For example, artistic license requires some

57 See Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule at Pt 1 (paras 1 and 2) and Pt 3 (paras 2–5). It also features in relation to the disclosure of personal data without consent for public interest in the Second Schedule at Pt 3 (paras 1 and 4).

58 [2016] SGPDPC 20.

59 *Eg*, it is unreasonable to store or keep personal data if such retention "is no longer necessary for legal or business purposes". See s 25 of the Personal Data Protection Act 2012 (2020 Rev Ed). See *eg*, *Re Social Metric Pte Ltd* [2017] SGPDPC 17, where the organisation retained the information beyond what was necessary for its legal or business purposes (at paras 28–29). It is of interest to note how the PDPC also used "necessary security measures" in lieu of the statutory phrase "reasonable security measures" in relation to the protection obligation under s 24 of the Personal Data Protection Act (at paras 32 and 33).

60 And it is not prohibited under s 14(2)(*a*) of the Personal Data Protection Act. See *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (Personal Data Protection Commission Singapore, 9 October 2019) at para 2.3.

flexibility and the exception from seeking consent for data collection for "artistic or literary purposes" can be considered necessary to meet the objective.[61] Similarly, the exception for the management of information relating to employment, business or profession is necessary for their specific purposes.[62]

31 These exceptions are also not exclusive and do not prevent the assessment from being made on a case by case basis where none of the exclusions apply.[63] As noted previously, it may in fact be justified and necessary *to not seek consent* (as opposed to not seeking consent) in some circumstances, such as where it may compromise investigations or proceedings (as it may affect the availability or accuracy of the personal data), and where it will not be forthcoming as the nature of the information will be prejudicial to the individual concerned.[64]

32 In *Re M Stars Movers & Logistics Specialist Pte Ltd*,[65] the PDPC stated that:[66]

> An organisation should not be prevented or hampered from responding to comments about it using the same mode of communications that its interlocutor has selected. In some situations, it may be reasonable or even necessary to disclose personal data in order to advance an explanation. An individual who makes false or exaggerated allegations against an organisation in a public forum may not be able to rely on the PDPA to prevent the organisation from using material and relevant personal data of the individual to explain the organisation's position on the allegations through the same public forum.

33 In this case, the PDPC also used the proportionality test to assess reasonableness:

> The following observations may be made in this context about the approach that the Commission adopts. First, the Commission will not engage in weighing allegations and responses on golden scales in order to establish proportionality. The better approach is to act against disclosures that are clearly disproportionate on an objective standard before the Commission intervenes in what is essentially a private dispute (in this case the dispute was the Complainant's alleged dissatisfaction with the services provided by the Organisation). Second, the disclosure may sometimes be justified by exceptions to consent. For example, disclosures in the course of the organisation's investigations into alleged breaches of agreement or into conduct that may give rise to tortious claims. Disclosures in reliance on exceptions to consent will nevertheless

61 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule at Pt 2, para 3.
62 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule at Pt 3, para 9.
63 *Eg*, see *Jump Rope (Singapore)* [2016] SGPDPC 21.
64 See *Jump Rope (Singapore)* [2016] SGPDPC 21.
65 [2017] SGPDPC 15.
66 *Re M Stars Movers & Logistics Specialist Pte Ltd* at [2017] SGPDPC 15 at [18].

> have to be limited in scope in order to achieve the purposes of the applicable exception. Third, even in the absence of consent (whether express or deemed) or an applicable exception, it may nevertheless be objectively reasonable for the organisation to disclose personal data in response to allegations made against it. Section 11(1) of the PDPA exhorts organisations in discharging its responsibilities under the PDPA to '*consider* what a reasonable person would consider appropriate *in the circumstances*.' [emphasis in original]. This requires fact-specific analysis and the burden is on the organisation to justify that the circumstances were atypical, the disclosure was warranted and its actions were reasonable.

34 The necessity standard also appears in other data protection laws. In the EU's GDPR, for example, the processing of personal data can be done without consent if it "is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract; … for compliance with a legal obligation to which the controller is subject; [… or] for the purposes of the legitimate interests pursued by the controller or by a third party [if certain conditions are met]".[67]

B. Practicability

35 This test has been used in the data protection laws of some countries in lieu of or synonymous with the "reasonableness" criteria.[68] The perspective is from the data collector's point of view. The difficulty of meeting its obligations is not necessarily a legitimate or legal excuse for non-compliance with an obligation, but it can still be a relevant factor under certain circumstances. This factor will be considered in more detail in relation to the legislative treatment of personal data in Hong Kong in Part V of this article.

36 It can be argued that practicability is also the basis for excluding the management of information by public agencies, and for the personal and domestic purpose or capacity exceptions from the general scope of the Act.[69] It is also not practicable to require consent for the collection, use or sharing of data that is already publicly available generally,[70] although specific unlawful uses, such as for the purpose of harassment by

67 GDPR Art 6(1). See also recitals 47 to 49 for examples of what may constitute "legitimate interest", which includes fraud prevention, direct marketing, affiliated organisations and cyber security.

68 For example, the Hong Kong Personal Data (Privacy) Ordinance (Cap 486) provides for a "reasonably practicable" test, which is defined according to a "reasonableness" measure. This is further examined in Part V of this article.

69 Personal Data Protection Act 2012 (2020 Rev Ed) s 4(1)(*a*).

70 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule at Pt 2, para 1.

doxxing or to commit computer offences and cybersecurity attacks, can be specifically legislated against.[71]

37 The research exception from consent under the PDPA states that an organisation may *use* personal data for a research purpose (including historical or statistical research) if certain conditions are met: "(a) the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form; (b) there is a clear public benefit to using the personal data for the research purpose; (c) the results of the research will not be used to make any decisions that affects the individual; and (d) in the event that the results of the research are published, the organisation publishes the results in a form that does not identify the individual".[72] An organisation may only *disclose* personal data for a research purpose (including historical or statistical research) if a different set of conditions are met: "(a) the research purpose cannot reasonably be accomplished unless the personal data is disclosed in an individually identifiable form; (b) it is impracticable for the organisation to seek the consent of the individual for the disclosure; (c) there is a clear public benefit to disclosing the personal data for the research purpose; (d) the results of the research will not be used to make a decision that affects the individual; and (e) in the event that the results of the research are published, the organisation publishes the results in a form that does not identify the individual".[73] It is noteworthy that the second limb of the exception for disclosure provides that it must be "impracticable" for the organisation to seek the consent of the individual for the disclosure of his or her personal data for the purpose of that research.

38 Furthermore, the test of practicability can also explain the limitation of the Act to the data of the deceased person to certain types of obligations and to within ten years of the subject's death as well as in limiting the PDPA's protections to recorded personal data for up to 100 years only.[74] It is also the basis for the apportionment of obligations between an organisation and a data intermediary with whom it has a contractual relationship for the processing of personal data on its behalf

71 See *eg*, s 3(1)(*c*) of the Protection from Harassment Act 2014 (2020 Rev Ed), s 9 ("Supplying, etc., personal information obtained in contravention of certain provisions") of the Computer Misuse Act 1993 (2020 Rev Ed) and the Cybersecurity Act 2018 (Act 9 of 2018) generally.

72 Personal Data Protection Act 2012 (2020 Rev Ed) Second Schedule at Pt 2, Div 3, para 1.

73 Personal Data Protection Act 2012 (2020 Rev Ed) Second Schedule at Pt 3, Div 2, para 1.

74 Personal Data Protection Act 2012 (2020 Rev Ed) s 4(4).

or for its purposes;[75] and for the redefinition of the responsibility of the organisation in this context.

39 Practicability is especially relevant in countries that equally value business needs and concerns. Hence, for example, correction of personal data is only required to be done "as soon as practicable" and not necessarily with immediate effect.[76] Even notification of data breaches need not be immediate, given the rationale for a reasonable delay may include "practical" concerns such as to aid in investigations, to prevent further leaks and to avoid destabilising the economy.[77]

40 In a PDPC's public consultation paper, when the Commission had sought views on the proposed deemed consent by notification, the consideration of whether it would be "impractical to obtain consent" was suggested as a condition.[78]

C. Proportionality

41 One example of the use of the "proportionality test" is the factoring in of an individual's "objective expectation of privacy" when determining the appropriateness of an organisation's purpose.[79] Thus, collecting contact information for complementary follow up services may be appropriate, but collecting the same information for marketing non-related products may not be. Another example is the risk assessment for data use in some of the statutory exceptions (*ie*, adverse effects assessment for the legitimate interest and deemed consent by notification exceptions).

42 Other examples of where the scales of proportionality may weigh against the need to obtain consent for personal data include situations where the effort to obtain consent and/or provide notification is particularly onerous whereas the organisation's purpose is innocuous,

75 Personal Data Protection Act 2012 (2020 Rev Ed) s 4(2)(3).

76 Personal Data Protection Act 2012 (2020 Rev Ed) s 22(2)(*a*).

77 Part VIA of the Personal Data Protection Act 2012 sets out the conditions for the mandatory notification of data breaches to the Commission and the "affected individuals". Due to the different objectives and concerns for the notification of the Commission and individuals, the conditions and procedures for notification are different. See also, Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021).

78 See *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (Personal Data Protection Commission Singapore, 27 July 2017).

79 In *Re My Digital Lock Pte Ltd* [2018] SGPDPC 3 at [39], the PDPC stated that "[i]n determining the appropriateness of any particular purpose, considerations of the data subject's objective expectation of privacy may conceivably be entertained".

and where timeliness is essential whereas the organisation's purpose is of great importance (such as on the basis of public interest).

43 In *Re Black Peony*,[80] the PDPC dismissed a complaint made by an individual against an organisation on the basis of bad faith and that there was no non-compliance with the consent obligation under s 13 of the PDPA. It stated that:[81]

> … where an individual chooses to engage an organisation publicly, there can be circumstances where the use or disclosure of personal data may be made without consent if it would be reasonable to do so. This may include situations where an individual makes an allegation or complaint against the organisation publicly but it is reasonable to expect that consent for the organisation to use the individual's personal data to respond to the allegations would not be forthcoming.
>
> Although it may be reasonable for the organisation to use and disclose personal data without consent or notification in certain situations, the Commission would emphasise that *in line with the standard of reasonableness that underpins the PDPA, any such use or disclosure of personal data should be proportionate and be limited to what is reasonable* for the organisation to respond to the individual's allegations and complaints.
>
> In this case, the Complainant chose to post her comments and engage the Organisation over the unsatisfactory service she received from the Organisation in publicly accessible posts online. Based on the Organisation's response on the blog and forum, there was nothing to show that the Organisation had been excessive or unreasonable in the use or disclosure of the Complainant's personal data.
>
> [emphasis added]

44 Similarly, in *Re M Stars Movers*,[82] beyond what was said on proportionality that was cited above, the PDPC further stated in relation to the use and disclosure of personal data in the context (and in relation to the appropriate forum) of a dispute that:[83]

---

80 [2017] PDP Digest 218.

81 *Re Black Peony* [2017] PDP Digest 218 at [7]–[9].

82 [2017] SGPDPC 15.

83 *Re M Stars Movers* [2017] SGPDPC 15 at [18]–[19]. Cited and applied in *Re My Digital Lock Pte Ltd* [2018] SGPDPC 3 at [7] where the PDPC "reiterate[d] that an organisation cannot be prevented from making *reasonable and proportionate responses* to defend itself from allegations made against it, even if personal data are disclosed in doing so" [emphasis added] (in relation to the exercise of its power to investigate a complaint). It was also cited and applied in *Re Big Bubble Centre Pte Ltd* [2018] SGPDPC 25 at [11]–[12], in relation to the s 13 consent obligation to the disclosure of personal data on social media in the context of a dispute between the organisation (employer) and an individual (ex-employee).

> The Deputy Commissioner advises caution in disclosing personal data when responding to public comments. An organisation should not be prevented or hampered from responding to comments about it using the same mode of communications that its interlocutor has selected. In some situations, it may be reasonable or even necessary to disclose personal data in order to advance an explanation. An individual who makes false or exaggerated allegations against an organisation in a public forum may not be able to rely on the PDPA to prevent the organisation from using material and relevant personal data of the individual to explain the organisation's position on the allegations through the same public forum.
>
> … the Commission will not engage in weighing allegations and responses on golden scales in order to establish proportionality. The better approach is to act against disclosures that are clearly disproportionate on an objective standard before the Commission intervenes in what is essentially a private dispute …

45 There is also a "disproportionate or unreasonable exception" to the general obligation on an organisation to provide an individual access to his or her personal data that is within the organisation's possession and control "where the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest".[84]

46 A benefit and detriment analysis primarily relates to the impact on the individual. Hence, for example, the "data protection impact assessment" is useful to determine whether the systems and processes in relation to data governance and management meet the protection obligation standard.[85] The specificity, that is, using only what is required

---

84 Personal Data Protection Act 2012 (2020 Rev Ed) Fifth Schedule at para 1(*j*)(ii). It may also be noted that the impracticability to satisfying such a request also provides an exception, that is, "for information that … cannot be found" or in relation to "any request that would unreasonably interfere with the operations of the organization". Personal Data Protection Act 2012 (2020 Rev Ed) Fifth Schedule at paras 1(*j*)(iii) and 1(*j*)(i) respectively.

85 *Guide to Data Protection Impact Assessments* (Personal Data Protection Commission, 14 September 2021) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.ashx?la=en> (accessed 7 February 2022). Similarly, in its *Advisory Guidelines on Enforcement of the Data Protection Provisions* (Personal Data Protection Commission Singapore, 1 February 2021) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.ashx?la=en%3EFeb-2021.ashx?%3Ela=en> (accessed 7 February 2022), the PDPC stated that it will take into account factors such as the seriousness and impact of a breach, the type and level of safeguards put in place (in proportion to potential harm), and whether it involved sensitive data (and the possible negative repercussions for the data subject) in determining whether to mete out a financial penalty and on the severity of the penalty. See also, *Central Depository (Pte) Limited* [2016] SGPDPC 11 and *Aviva Ltd* [2016] SGPDPC 15 on the sensitive nature of the data *vis-à-vis* the directions to be imposed.

and no more than that in meeting the objectives of an organisation, is also relevant to a proportionality assessment. Indeed, this is central to the purpose limitation obligation and is key to meeting that core obligation.[86]

47 A proportionality assessment is also explicitly built into the unilateral "legitimate interest" assessment for dispensing with consent (First Schedule, Pt 3) by the data controller (and to some extent in the research exception under the Second Schedule, Pt 2, Div 3 and Pt 3, Div 2 in relation to use and disclosure respectively). This is unlike the case of deemed consent by notification which permits the data subject to "opt-out".

48 Finally, it is worth noting that the GDPR has, as one of its core principles, the need for "fairness" and "proportionality" in the processing of personal data.

D. Reasonableness in relation to other obligations

49 The below table sets out how the reasonableness assessment is taken in relation to specific statutory obligations. The relevance of the factors determining reasonable conduct will vary between statutory commitments.

Provision (Obligation)	Obligation (and factors of analysing reasonableness, if any)
Section 15 Deemed consent for the collection, use or disclosure of personal data	An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if the individual, without actually giving consent referred to in s 14, voluntarily provides the personal data to the organisation for that purpose; and it is reasonable that the individual would voluntarily provide the data.

86 Personal Data Protection Act 2012 (2020 Rev Ed) s 18.

Provision (Obligation)	Obligation (and factors of analysing reasonableness, if any)
Section 15A Deemed consent by notification for the collection, use or disclosure of personal data	The organisation must, before collecting, using or disclosing any personal data about the individual: (a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual; (b) take reasonable steps to inform the individual of the organisation's intention and purpose and provide for a reasonable period within which, and a reasonable manner by which, the individual may deny (withdraw) consent; and (c) identify and implement reasonable measures.
Section 18 Limitation of purpose and extent	An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and the individual has been informed or notified, if applicable.
Section 20 Notification of purpose	An organisation shall inform the individual of the purpose for the personal data and provide a point of contact for further inquiries.
Section 21 Access to personal data	On the request of an individual, an organisation shall, as soon as reasonably possible provide to the individual information about personal data within its possession or control and how it has been used or disclosed (Sched 5 exceptions or limitations in line with categories of specific statutory exceptions to consent).
Section 22 Correction of personal data	An organisation shall correct the personal data in its possession or under its control as soon as practicable after receiving a request to do so by an individual, unless the organisation is satisfied on reasonable grounds that the correction should not be made. The correction shall be made as soon as practicable (Sched 6 exceptions or limitations in line with categories of specific statutory exceptions to consent).

Provision (Obligation)	Obligation (and factors of analysing reasonableness, if any)
Section 23 Accuracy of personal data	An organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or is likely to be disclosed by the organisation to another organisation.[87]
Section 24 Protection of personal data[88]	An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored.
Section 25 Retention of personal data	An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes.

Table 2. The "reasonableness text" and the personal data protection obligations

87 It may be noted how the "effects" and impact doctrine is used in the GDPR to determine the scope of personal data instead, and how a similar measure of adverse effects appear in some of the PDPA's statutory exceptions, notably legitimate interests, and deemed consent by notification.

88 Daniel Foo Ee Yeong, "Suggestions on the Relevance of the Organization's Size to Section 11 of Singapore's Personal Data Protection Act" *Singapore Law Review* <http://www.singaporelawreview.com/juris-illuminae-entries/2018/suggestions-on-the-relevance-of-the-organizations-size-to-section-11-of-singapores-personal-data-protection-act> (accessed 7 February 2022).

IV. The Personal Data Protection Act 2012's "reasonableness" standard and the "fair use" as permitted use to copyright infringement

50 To better understand the integral nature of the "reasonableness test" to the nature and objective of the PDPA, it will be useful to compare it to the fair use exception in the Singapore copyright regime.

51 The current "fair use" provision in the SCA[89] in substance operates as a broader exception than the "fair dealing" exception that was the original provision in the SCA. It is essentially drawn from and the same as the open-ended "fair use" exception under the United States' Copyright Act.[90] This has in fact been so in substance, if not in "form" (*ie*, it was still referred to as "fair dealing"), since the original provision (the old s 35) was amended in 2004 with that purpose in mind, but have been made explicitly so in the 2021 amendments:[91]

> The open-ended nature of the Singapore exception is also more akin to the notion of 'fair use', where the exception is more general in nature and not restricted to only certain uses or activities. Given these similarities with 'fair use', the exception should be more accurately called 'fair use'. We note this already coincides with the current general understanding and practice, where the Singapore exception is commonly seen as an adaptation of the US 'fair use' defence. However, this will be purely a change in terminology; we do not suggest that American jurisprudence will now be more persuasive as a result of calling the exception 'fair use'. As was observed by the Singapore Court of Appeal, the underlying factors in Singapore's exception are of Australian origin and the first four factors also mirror the US 'fair use' factors, so both American and Anglo-Australian jurisprudence will be helpful in shaping the law in this area.

52 The open-ended general "fair use" exception in the SCA is supplemented by other statutorily listed specific exceptions that are considered fair based on the nature of the use and the public policy objectives that they seek to achieve that trump what are essentially private rights to copyrighted materials.[92]

---

89 Copyright Act 2021 (Act 22 of 2021), which entered into force on 21 November 2021.

90 Copyright Act 2021 (Act 22 of 2021) s 190 and 17 USC (US) §107 (1976) respectively.

91 *Singapore Copyright Review Report* (Ministry of Law Singapore & Intellectual Property Office of Singapore, 17 January 2019) at para 2.6.8.

92 See Pt 5, Div 2 of the draft Copyright Amendment Bill of 2021, available at: <https://www.mlaw.gov.sg/files/news/public-consultations/2021/copyrightbill/Annex_B-CopyrightBill.pdf> (accessed 7 February 2022). See also Pt 1 of *Public Consultation on the Proposed Copyright Bill* (Ministry of Law & Intellectual Property Office of Singapore, 5 February 2021) at para 27, available at: <https://www.mlaw.gov.sg/files/news/public-consultations/2021/copyrightbill/Copyright_Consultation2021.pdf> (accessed 7 February 2022).

53 In comparison to the doctrine of "fair use", the PDPA reasonableness criteria is equivalent to the SCA fairness criteria and functions in much the same way, to achieve a similar objective of providing a fair apportionment of rights in relation to information (defined and referred to as "personal data" and copyrightable "original works" respectively) between societal stakeholders with an interest in its protection or use.

54 "Reasonable" is defined as "having sound judgment; fair and sensible" or "as much as is appropriate or fair" in the Oxford Dictionary,[93] and as something "based on or using good judgment and therefore fair and practical" in the Cambridge dictionary.[94] It is noteworthy that the words "fair" (as applied to a situation where conflicting interests may arise) and "appropriate" (taking into account the profile of the parties, the nature of the personal data, its purpose and the obligation concerned as well as the socio-cultural norms of the times) appear in these definitions. In the exercise of such judgment, decisions must be made rationally and objectively, taking into account the interests of the data user-controller and subject. Hence, the perspective of a judge or impartial arbiter, such as a data commissioner, will be the most appropriate one to take when assessing each situation.

55 Unlike the "reasonable man" test in tort law which is concerned with managing human behaviour and expectations in society, both the "reasonableness text" in copyright and data protection law deal with the uniqueness of data that is closely linked to a person's individuality and personality. In relation to the former, originality is a requirement for copyright protection while uniqueness is a feature of personal data. These laws serve to provide property-like rights and protections to safeguard and balance these interests in the face of conflicting socio-economic interests as well as the rights and interests of other data users. Reasonableness is key to such an exercise. These rights include precluding others from accessing and using the data concerned without permission generally and to control its use and dissemination subject to exceptions that cater to other societal and stakeholder interests.

93 See the Oxford Learner's Dictionaries website: <https://www.oxfordlearnersdictionaries.com/> (accessed 7 February 2022).

94 See the Cambridge Dictionary website: <https://dictionary.cambridge.org/> (accessed 7 February 2022).

A. Statutory exceptions: Mandatory requirements or factors and guidelines or considerations

56 The "reasonableness text" is also flexible, and depending on the statutory obligation, can incorporate an assessment of different measures, as noted earlier. In the same way that the PDPA's statutory exceptions are considered reasonable based on the objective of the personal data processing, the copyright fair use doctrine is supplemented by a list of purpose-based exceptions that are deemed fair by nature of their use or function, sometimes with a set of conditions to maintain the fairness of the use. These statutory exceptions can also be amended from time to time. As noted, for instance, the PDPA was amended in 2021 to re-categorise pre-existing exceptions and also to include new ones; while the SCA now also provides for new purpose-based exceptions which include: (a) facilitating the use of works for text and data mining; (b) allowing for educational uses relating to non-profit educational institutions; and (c) supporting the work of galleries, libraries, archives and museums (all of which includes conditions for the exception to apply, to safeguard and maintain fairness of use).[95] It is also made clear that these exceptions are "permitted uses" that do not constitute an act of infringement, and they are also independent (and not mutually exclusive) of the general fair use exception and "does not limit" it in any way (*ie*, an act may fail the conditions for a potentially relevant specific exception to apply but nevertheless pass the general fair use analysis).[96] Similarly, a collection, use or sharing of personal data without consent may not fall under a statutory exception but can nevertheless be done without permission if it was reasonable to do so, albeit the onus is for the party arguing fair use or reasonableness to prove that it is so in relation to the SCA and the PDPA respectively. Moreover, and similar to the role and status of the fair use exception under the SCA, if the act relating to personal data is reasonable under the PDPA, then it acts as a justification rather than as an excuse from compliance with the relevant obligation. For that reason, complainants and the PDPC should consider the reasonableness of the act of data collection, use or disclosure when lodging a complaint and when proceeding with an investigation respectively.[97]

---

95 See Pt 5, Div 8, cll 195 and 76(*a*), and Pt 5, Div 6 of the draft Copyright Amendment Bill of 2021 respectively. See *Public Consultation on the Proposed Copyright Bill* (Ministry of Law & Intellectual Property Office of Singapore, 5 February 2021) at paras 28–31.

96 Clauses 176–177 of the draft Copyright Amendment Bill of 2021. See *Public Consultation on the Proposed Copyright Bill* (Ministry of Law & Intellectual Property Office of Singapore, 5 February 2021) at para 42.

97 Personal Data Protection Act 2012 (2020 Rev Ed) s 50. See also, *Re My Digital Lock Pte Ltd* [2018] SGPDPC 3.

57 Many of the considerations and statutory factors are similar, such as the purpose and nature of the data use (encompassing both public policy and private interest components), the commerciality of the use (in contrast to socially beneficial or personal use), and the nature of the data or content (*eg*, sensitive or valuable and its impact on the individual). Table 3 sets out the similar considerations and factors for the SCA fair use and the PDPA "reasonableness text" in the context of the general compliance obligation under the respective regimes:

Considerations or factors	How is the use fair? (Part 5 of the SCA)	When is not obtaining actual consent reasonable?
Open-ended exception (or permitted use)	Division 2 Section 190 (general) inherent in this is a balance of interest assessment, with public and private considerations; which shall include the following (non-exhaustive) considerations when considering fair dealing or fair use:[98]	Section 11 (general) is it reasonable *vis-à-vis* the individual and the organisation?[99] (*ie*, a balance of interest assessment, with public and private considerations) • Section 15(1)–15(2) (deemed consent) is it related to the purpose and will there be objections if it was posed to the individual?[100]

98 Copyright Act 2021 (Act 22 of 2021) s 191. In contrast, there are no mandatory factors for the "reasonableness text", although there are different factors or assessment checklists for specific exceptions within their respective sub-provisions including, and in particular, for the legitimate interests and deemed consent by notification exceptions (that notably either provide for a balance of interests, reasonableness and/or appropriateness evaluation or both). However, as this list is non-exhaustive, and have indeed been amended and adapted over time, such as the inclusion (and proposed deletion) of the fifth factor ("(e) the possibility of obtaining the work or adaptation within a reasonable time at an ordinary commercial price") and the development of the "transformative use" doctrine in relation to the first factor in US copyright jurisprudence respectively.

99 Personal Data Protection Act 2012 (2020 Rev Ed) s 11.

100 Personal Data Protection Act 2012 (2020 Rev Ed) s 15.

Considerations or factors	How is the use fair? (Part 5 of the SCA)	When is not obtaining actual consent reasonable?
	(a) the purpose and character of the dealing, including whether such dealing is of a commercial nature or is for non-profit educational purposes; (b) the nature of the work or adaptation; (c) the amount and substantiality of the part copied taken in relation to the whole work or adaptation; and (d) the effect of the dealing upon the potential market for, or value of, the work or adaptation.	• Section 15A (deemed consent) will notification suffice?[101] • Legitimate interests exception (broad exception).[102] • Is there valid business or legal reasons to do so (*eg*, informing of a person's dismissal or blacklisting from a company) and where consent is unlikely to be forthcoming?[103] • Is it to report an offence or malpractice for purpose of criminal investigation or internal disciplinary process (*eg*, such as not to alert the alleged offender to preserve evidence and as consent is unlikely to be forthcoming)?

101 Personal Data Protection Act 2012 (2020 Rev Ed) s 15A.

102 According to *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (Personal Data Protection Commission Singapore, 1 October 2021) at para 12.63, examples of legitimate interests "include the purposes of detecting or preventing illegal activities (*eg*, fraud, money laundering) or threats to physical safety and security, IT and network security; preventing misuse of services; and carrying out other necessary corporate due diligence. Subjecting such purposes to consent is not viable as individuals may choose not to give consent or to withdraw any consent earlier given (*eg*, individuals who intend to or who had engaged in illegal activities), impeding the organisations' ability to carry out such functions".

103 See *Jump Rope (Singapore)* [2016] SGPDPC 21 at para 10. The example is given of a situation where there was credible evidence of fraudulent conduct such as where a former employee misrepresents his status of employment and association with his former employer. In such a case, the Commissioner opined that it may be reasonable for the former employer to inform existing customers informing of the facts. However, the latter should still notify the former of the communication to be made to the existing customers, so that the disclosure of personal data is made transparent: see *Jump Rope (Singapore)* [2016] SGPDPC 21 at para 11.

Considerations or factors	How is the use fair? (Part 5 of the SCA)	When is not obtaining actual consent reasonable?
Specific exceptions (explicitly stated as a form of fair use and with conditions)	Division 2 Section 192 For the purpose of reporting news, with sufficient acknowledgement if not impracticable	• Matters affecting the public • Public interest exception
	Division 2 Section 193 Purpose of criticism or review of that work or another work (can include parody or satire)	
	Division 2 Section 194 Purpose of research and study, with restriction that a reasonable portion of an article is used	
Specific exceptions (not explicitly stated as a form of fair use and with conditions, but nevertheless justified on the basis of fair use based on policy grounds)	Public interest (including societal interest and some elements of individual's interest in some cases): Division 3 Education and Educational Institutions Division 4 Persons with Print Disabilities Division 5 Persons with Intellectual Disabilities Division 6 Public Collections: Galleries, Libraries, Archives and Museums	• Matters affecting the public • Public interest exception • Research
	Business and technological innovation and function (elements of individual's interest in some cases): Division 7 Use of Computer Programs Division 8 Computational Data Analysis	• Section 15(3)–15(10) (deemed consent) by contractual necessity • Legitimate interests exception • Business asset transaction exception • Business improvement exception • Research exception

Considerations or factors	How is the use fair? (Part 5 of the SCA)	When is not obtaining actual consent reasonable?
Individual's interest (emergency only, involving matters relating to health, safety and death)	N.A.	Vital interests

Table 3. Comparison of the Copyright Act 2021's fair use exception and the Personal Data Protection Act 2012's reasonableness standard of compliance

58 The considerations for the apportionment of rights and interests, in relation to the access and use of personal data as valuable asset, is not so different from that which relates to the access and use of creative works in copyright law. Hence, the factors and tests that are used to determine fairness can likewise be used, albeit modified to suit the context, to determine what is reasonable in any given situation. A general comparison of these factors in assessment is set out in Table 4:

Factors assessing fair use not constituting an infringement of the copyright in a creative work[104]	Factors determining reasonableness of acts in relation to personal data (especially that relating to purpose limitation and consent)
The purpose and character of the dealing, including whether such dealing is of a commercial nature or is for non-profit educational purposes.	The purpose of the data collection, the type of use or the objective of the sharing and with whom; also, whether it is used for commercial gain can also be relevant as it may be objectionable to the data subject (unless, for example, there is sufficient notice and/or remuneration; requiring separate consent for marketing purposes is a good example of the reasonable extent of consent collected in a commercial transaction).
The nature of the work or adaptation.	The nature of the personal data such as whether it is sensitive data.
The amount and substantiality of the part copied taken in relation to the whole work or adaptation.	The data should be evaluated individually or as a bundle depending on the objective of the data controller.

104 Copyright Act 2021 (Act 22 of 2021) s 191.

The effect of the dealing upon the potential market for, or value of, the work or adaptation.	The value of the personal data can also be a consideration, especially if personal data is viewed as a form of personal property.
The possibility of obtaining the work or adaptation within a reasonable time at an ordinary commercial price.[105]	The inconvenience, cost and labour required to obtain actual consent and how bothersome and inefficient it may be to the data subject (the deemed consent by notification is clearly a fair compromise developed for this purpose).

Table 4. Compatibility of the mandatory factors determining fair use with the assessment of reasonableness

59 A reasonableness assessment can take into account public interest and also data interests and rights of others besides the organisation and individual concerned. Hence, the PDPA is subject to other laws relating to data that includes personal data.[106]

B. Statutory exception: A right and not a defence – prima facie *good faith assessment by complainants and the commissioner*

60 Following from the above observation that there is no infringement *ab initio* where there is a permitted use or statutory exception (*ie*, they function as a right that negates infringement or non-compliance, as the case may be), and that these doctrines do not act as a defence but serve as a right,[107] in practice, to utilise the general open-ended fair use or reasonableness exception, the evidential burden of proof rests on the user at the very least.

105 This factor has been removed from the provision under the 2021 amendment, but it remains useful as a non-mandatory consideration where relevant and appropriate.

106 See s 4(6) of the Personal Data Protection Act 2012 (2020 Rev Ed), which states that the data protection obligations (including the consent obligation to the collection, use and disclosure of personal data by an organisation), shall not affect "any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening this Act; and the provisions of other written law shall prevail to the extent that the [statutory obligations, including the consent obligation, are] inconsistent with the provisions of that other written law".

107 See Warren Chik, "Better a Sword Than a Shield: The Case for Statutory Fair Dealing/Use Right as Opposed to a Defence in the Light of the Disenfranchising Effect of Digital Rights" (2008) *International Journal of Private Law* 1.

61 It may be noted that because fair use is not considered infringing conduct and is an authorised exception rather than an excuse, in the United States, the Court of Appeal for the Ninth Circuit determined in the context of *Lenz v Universal Music Corp*[108] ("*Lenz*") that the copyright owner is required to make an initial and proper fair use assessment before filing a takedown notice to an Internet intermediary that is a service provider (in that case, YouTube). In such a case, lacking a clear indicator of a permissible form of use (unlike the statutory listed exceptions), a good faith consideration of fair use at the very least (but perhaps not necessarily an in-depth or time consuming assessment or analysis, given how onerous and complex it can be) is required for the copyright owner to defend against an allegation of misrepresentation.[109] It is unclear if this "duty" will be similarly placed on the copyright owners in the Singapore context since, unlike the United States' Copyright Act,[110] the Singapore Copyright Act does not provide for a cause of action against a copyright owner which misrepresents that the materials in a takedown notice are infringing or that had not made a good faith consideration of fair use before action is taken against an alleged infringer.

62 In comparison, the onus of proving reasonableness of action (despite not being exempted specifically in the Act) still lies on the organisation if the complaint is sent to the PDPC administrative panel or to the courts (or for alternative dispute resolution). However, unlike *Lenz*, in the context of the PDPA, the complainant is the individual data subject whereas the defendant is the organisation (including persons) processing his or her personal data.[111] Hence, resource-wise, the respondent to a complaint is generally in a better position to justify a use and deal with a complaint under the data protection regime. Moreover, it may be noted that the PDPC's powers to investigate include a broad discretion to suspend, discontinue or refuse to investigate complaints, including on the basis of complaints "not made in good faith" (and also those that are "frivolous" or "vexatious", which can include making complaints knowing that there is an applicable exception or despite the apparent reasonableness of the act), which may include considering

108 801 F 3d 1126 (9th Cir, 2015), affirming the District Court for the Northern District of California's ruling that copyright owners must consider fair use in good faith before issuing a takedown notice for content posted on the World Wide Web.

109 17 USC (US) §512(f) of the Digital Millennium Copyright Act ("DMCA"). See, Amanda Schreyer, "Misrepresentation Under the DMCA: The State of the Law" (2014) 25(1) NYSBA Entertainment, Arts and Sports Law Journal 72; "*Lenz v. Universal Music Corp.*: Ninth Circuit Requires Analysis of Fair Use Before Issuing of Takedown Notices" (2016) 129 Harv L Rev 2289.

110 17 USC (US) §107 (1976).

111 In relation to copyright disputes, the complainant is more often than not (although not restricted to) a legal entity while the defendants are more often individuals.

the reasonableness of the data collection, use or sharing before lodging a complaint and commencing proceedings.[112] It is recommended that there should be some form of penalty for complainants that abuse the process and make frivolous, vexatious or bad faith complaints to stifle business interests.

63 That said, placing at least the evidential burden of proof on the organisation in the context of the PDPA is the correct approach as: First, it will not be consistent with the personal data protection to require an individual that is unlikely to know or understand the compliance standard, which is placed on the organisation. Second, the profile of the organisation, the facts and circumstances relating to the collection, use or disclosure of the personal data, the purpose and other unique considerations are privy to the organisation, and hence it is in the best position to make the assessment of reasonableness and provide proof. Third, the duty rests on the organisation to comply with the obligations under the Act; however, as noted, the PDPC can exercise its discretion not to proceed with an investigation, initiated by a complaint (or of its own motion), based on a list of circumstances including on the basis that the complaint is "frivolous or vexatious or is not made in good faith" (a similar consideration as an action for misrepresentation under the US Copyright Act, but without liability). Fourth, a complaint cannot be "weaponised" against organisations as complaints are brought to the PDPC that actively considers all the facts of the case, as opposed to a copyright infringement complaint and takedown notice issued to a private entity (*ie*, an Internet intermediary or service provider) that can be abused and that may not fairly and effectively safeguard the interests of all the parties concerned in the dispute, including the complainee (*ie*, it could be "weaponised" against the interests of the individual under copyright law and take away their "right" to fair use).[113]

C. Additional observations

64 Despite the above comparison and similarities (especially relating to the purpose of the data collector or user), there are some differences between the SCA fair use doctrine and the PDPC reasonableness

112 Personal Data Protection Act 2012 (2020 Rev Ed) s 50(3)(*e*)(i). See also *Re My Digital Lock Pte Ltd* [2018] SGPDPC 3 at [53].

113 Appeals can only be made to the High Court after the decision of the Data Protection Appeal Committee (Part 9D Appeals) on specific grounds such as on a point of law arising from the latter's decision or direction, or from any direction relating to the amount of a financial penalty (s 48R(1) of the Personal Data Protection Act 2012). Also, the right of private action must be based on proof of loss or damage suffered as a direct result of a contravention of an organisation's obligations, the onus of which lies on the plaintiff (s 48O of the Personal Data Protection Act 2012).

standard. The fair use as a permitted use or "right" cannot be taken away or derogated from unless the circumstances and facts change rendering it "unfair" or the form of use have changed. This is understandable given that the fair use doctrine is very much focused on the nature and purpose of the use. On the other hand, as the reasonableness assessment is used to assess compliance with a wider swath of statutory obligations in the context of the PDPA (beyond the purpose limitation obligation), that may not always be so. For example, in relation to the consent obligation, an individual is given the ultimate right to withdraw consent given or deemed to have been given,[114] although reasonable collection, use or disclosure without consent *cannot* be withdrawn in certain situations, such as where it is statutorily not possible,[115] collection is required or authorised by law,[116] or in circumstances where the very reasonableness of not having to seek consent is on a basis that transcends the individual's interest or autonomy (*eg*, to investigate fraud, *etc*).

65 As an aside, it may be noted that even within the strict "closed list" system of the GDPR, the exceptions to consent must be applied in specific provisions in a manner to ensure that it is both "lawful" and "fair",[117] including in relation to "provisions relating to specific processing situations".[118]

V. The "reasonableness text" in the personal data protection laws of other jurisdictions

66 What is and is not "personal data" should be objectively ascertained and "value neutral", whereas what acts are "reasonable" when it comes to the management of personal information takes into consideration the facts and circumstances of each case. The Singapore PDPA's approach in treating what is "personal data" separately from the compliance standard based on the assessment of reasonableness provides much clearer guidance to the stakeholders.[119] This is not the case in the data protection laws in some other countries that obfuscate the

114 Personal Data Protection Act 2012 (2020 Rev Ed) s 16(1). See also, *Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7 at [13(b)].

115 Personal Data Protection Act 2012 (2020 Rev Ed) s 17 and the Scheduled exceptions to consent.

116 Personal Data Protection Act 2012 (2020 Rev Ed) s 16(4).

117 GDPR Art 6(2).

118 GDPR Chapter 9 (Arts 85–91).

119 Hence, the former is defined in s 2 without reference to any standard of compliance, which is separately outlined in s 11(1) generally and other sections of the Act in relation to (and in the unique context of) the obligation in question. In comparison to the Singapore Copyright Act 2021, it is similar to how the determination of what constitutes a copyrightable creative work is entirely different from the assessment of

(cont'd on the next page)

line between the two concepts and do not treat the inquiry as mutually exclusive. The latter approach has led to confusing, and in some cases, contradictory decisions. This can be illustrated by the decisions made by the Privacy Commissioner pursuant to the Hong Kong Personal Data (Privacy) Ordinance, which will be examined first, below.[120]

67 It is also not an ideal approach to make policy considerations on a case by case basis or to leave it to the administrative decision-maker or courts (as the case may be) to do so through the interpretation of "personal data". In relation to this, the PDPA's approach to supplementing the main and general compliance threshold with a carefully calibrated set of statutory exceptions based on policy grounds is preferable. In contrast, examples will be drawn from the European Court of Justice cases relating to similar disputes, specifically over the right of access to "personal data" by the data subject, which show the problem of leaving policymaking to the judiciary (and by extension, to administrative decision-makers) rather than to the legislature (through the use of statutory exceptions that can be amended from time to time).

A. "Personal data", practicability and the Hong Kong Personal Data (Privacy) Ordinance

68 By incorporating the "practicability" inquiry in the statutory definition of "personal data", the Hong Kong Personal Data (Privacy) Ordinance essentially fused (and confused) the scope of "personal data" with the standard of compliance and brought in considerations like the subjective intention of the data collector that should not be relevant.

69 Under the Hong Kong Personal Data (Privacy) Ordinance, "personal data (個人資料)" means "any data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable".

70 The word "practicable" appears twice in the definition of personal data and in different capacities.[121] First, the identifiability of the individual from the data in question must be practicable; and second, the personal data must be in a form that is practicable for access and processing. "Practicable" is defined as "reasonably practicable".[122] What is "reasonably

fair use, since the objectives for protection of such works and the exception are not the same.

120 Personal Data (Privacy) Ordinance (Cap 486) (HK).

121 Personal Data (Privacy) Ordinance (Cap 486) (HK) s 2.

122 Personal Data (Privacy) Ordinance (Cap 486) (HK) s 2.

practicable" is a question of fact and the test of "reasonableness" comes to the fore.

71 In a complaint to the Hong Kong Privacy Commissioner for Personal Data ("HKPC"), an individual complained against a public transport company on the basis that when he used his card to cross the toll gate, it triggered the lights and alarm, which in his opinion amounted to a disclosure of his personal data, revealing to the public that he was over 65 years old.[123] The HKPC determined that as the card could be purchased by anyone, the fact that the light and sound were emitted did not make it "reasonably practicable" for the identity of the complainant to be ascertained.

72 The relevance and intention of the data collector, *vis-à-vis* the data subject, was examined in greater depth in *Eastweek Publisher Limited v Privacy Commissioner for Personal Data*[124] ("*Eastweek*"). In this case, a complaint was lodged with the HKPC by a woman who was photographed by a tabloid magazine without her knowledge or consent. The photograph was subsequently published in the magazine with comments that were unflattering and critical of her dressing style that caused personal embarrassment to her (in particular in relation to people who know her such as her colleagues and clients). The HKPC decided that it contravened the Data Protection Principle 1(2)(b)[125] and the Court of First Instance dismissed the application for judicial review. However, the publisher appealed to the Court of Appeal, which reversed the Court of First Instance's decision by a simple majority. In the judgment, Justice Roberto Alexandre Vieira Ribeiro decided that there was no "collection" of "personal data" by the publisher although a photograph in which an individual can be identified is undoubtedly personal data.[126] In other words, the subjective intent of the data collector whether to identify or to seek to identify the person determines whether the Ordinance is applicable. The identity and identifiability inquiry, which forms part of the definition of personal data, is implicated in this analysis:[127]

123 *Kenneth Poon Sai-Ho v Privacy Commissioner for Personal Data* Administrative Appeal No 16/2000.

124 *Eastweek Publisher Limited v Privacy Commissioner or Personal Data* [2000] 2 HKLRD 83.

125 See Personal Data (Privacy) Ordinance (Cap 486) (HK) Schedule 1.

126 The judge accepted that a photograph is "data" and can be "personal data" despite the arguments for the appellant otherwise: *Eastweek Publisher Limited v Privacy Commissioner or Personal Data* [2000] 2 HKLRD 83 at p 18. Similarly, the dissenting judge found that a photograph is "data" and "personal data": *Eastweek Publisher Limited v Privacy Commissioner or Personal Data* [2000] 2 HKLRD 83 at pp 24–26.

127 *Eastweek Publisher Limited v Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83 at p 10 and 14. *Eg*, collection as part of a dossier or portfolio such as of "actors, entertainers or fashion models maintained by a theatrical impresario

(cont'd on the next page)

> … It is, in my view, of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify. …
>
> … In my view, many of the other provisions of the Ordinance and in the data protection principles can only operate sensibly on the premise that the data collected relates to a subject whose identity is known or sought to be known by the data user as an important item of information. …

73 In other words, in order for there to be an act of personal data collection, two conditions must be met: (a) the collecting party must be compiling information *about an* individual; and (b) the individual must be one whom the collector of information *has identified or intends or seeks to identify*; in other words, the identity of the individual must be *an important item of information to the collector*.

74 The judgment also further stated that the other obligations under the Ordinance only make sense if the data collector did so only in relation to the identified data subject (*eg*, for a purpose relating to or directed at the individual in question, such as an article about a celebrity or the use of data for targeted marketing).

75 It is submitted that the "reasonableness text" should be an objective one and not be based on a more arbitrary subjective inquiry similar to that taken in *Eastweek*.[128] Although the majority judges did distinguish between data collection and personal data, the conditions in effect deprive the data subject of the requirements and protections of the Ordinance simply because the determination of a lack of personal data collection will in reality obviate compliance with all the other data protection obligations under the Ordinance like a house of cards. In other words, collection itself is a condition for the other obligations to enter into effect. It cannot be said that there was no collection of personal data but yet, when the purpose of such determination relates to the obligations (such as to remove) or for remedies (such as damages) to apply, where relevant:[129]

---

or fashion modelling agency" or databases of wanted persons by law enforcement agencies where the identify and location of the person is important and sought after: *Eastweek Publisher Limited v Privacy Commissioner or Personal Data* [2000] 2 HKLRD 83 at p 17.

128 This approach has been applied to legitimise the installation and use of surveillance camera ("CCTV") systems that cover a semi-public or public area in the Hong Kong Administrative Appeals Board's ("HKAAB") decision in Administrative Appeal No 7/2019. In its decision, the HKAAB explained that it was bound by the *Eastweek* approach but expressed misgivings that the rule was outdated and construed the collection of personal data too narrowly.

129 *Data Protection Principles in the Personal Data (Privacy) Ordinance – From the Privacy Commissioner's Perspective* (Office of the Privacy Commissioner for Personal

(cont'd on the next page)

> Nevertheless, in none of those cases is the publisher or editor in question seeking to collect personal data in relation to any of the persons shown in the photographs and, in my view, the taking of such pictures and their use in such articles would not engage the data protection principles (whatever other liability, if any, such publication may attract).

76 This potentially deprives data subjects in Hong Kong of the protection of the entire Ordinance and is problematic on several fronts. It can extend beyond the taking of photographs by publishers as the type and form of data (*eg*, audio-visual recordings, online activities, *etc*) and types of data collected can be more varied. For example, collection of personal data through surveillance cameras ("CCTV"), and the processing of personal information (such as applying big data analytics and profiling techniques) for any "intention" other than collecting an individual's personal data is permitted.[130] Moreover, indirect identification, such as by third parties, are not relevant as well, and the effects or impact on the individual concerned becomes irrelevant.

Data, Hong Kong, 2nd Ed, 2010) at paras 3.19–3.21 <https://www.pcpd.org.hk/english/resources_centre/publications/books/files/Perspective_2nd.pdf> (accessed 7 February 2022). In Administrative Appeal No 24/1999, the complainant made a data access request for a copy of minutes kept by the data user as records of the meeting. The complainant attended the meeting and the subject matter covered in the minutes was about a report of a boiler accident. On appeal against the Commissioner's finding of no contravention, the Chairman of the AAB ruled that the contents of the minutes did not amount to the personal data of the complainant but was primarily concerned with the piece of equipment in question although it had recorded some of the remarks made by the complainant. The complainant applied for judicial review of the HKAAB's decision. In considering whether to grant judicial review in *Tso Yuen Shui v Administrative Appeals Board* HCAL 1050/2000, the Court of First Instance applied *Eastweek* and ruled that the minutes concerned issues arising from the maintenance and repair of the boiler only, and the identity of the complainant was not an important piece of information to the data user. In the circumstances, the Court ruled that the contents of the minutes did not contain the complainant's personal data. The decision of the Court of First Instance was affirmed by the Court of Appeal in CACV 960/2000. See *Personal Data (Privacy) Ordinance – From the Privacy Commissioner's Perspective* (Office of the Privacy Commissioner for Personal Data, Hong Kong, 2nd Ed, 2010) at para 3.16.

130 *Personal Data (Privacy) Ordinance – From the Privacy Commissioner's Perspective* (Office of the Privacy Commissioner for Personal Data, Hong Kong, 2nd Ed, 2010) at para 3.18. Contrast this to the EU approach in Judgment of 11 December 2014, *František Ryneš v Úřad pro ochranu osobních údajů*, C-212/2013, ECLI:EU:C:2014:2428, which included domestic CCTV that filmed a public area for security purposes generally under the EU Data Protection Directive and refused to exempt it based on the household exemption, available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=440706> (accessed 1 January 2020). In contrast, in Hong Kong, since the identity of the complainant neighbour was not the intention for the surveillance and not important to the data collector, it should not fall within the Ordinance.

77 The question also arises as to whether third parties that recognise the individual, collected that information from the initial source, and go on to *use* the data in relation to the data subject, are then subject to the Ordinance. On the one hand, if it is not personal data in the first instance, it should not "become" personal data down the chain of sharing or collection (*ie*, the original intention of collection "infects" the data and takes away the protection entirely). However, it seems more likely that it can be personal data subject to the Ordinance if the data collector's intention or identification fits the second condition for personal data collection, regardless of the source of such collection, since personal data need not originate (or be collected) from the data subject.[131]

78 In the Singapore PDPA context, the problem will likely be avoided by its exceptions. For example, the deemed consent by notification provision makes it reasonable to deem consent in cases where personal data in the form of photographs are taken, or recordings are made, during a public event. Another example is the use of the publicly available information exception can be used to exclude, from the ambit of consent requirement, the taking of photographs or filming in public areas that may capture the images of the people in the vicinity, who are not the main subject of the photograph or video in question, in the frame.

79 It will be clearer and provide for a more consistent approach to disputes for the legislature to produce statutory exceptions that take into consideration public policy interests that may conflict with the rights of individual data subjects (and the obligations of the data controller), than to leave these decisions to be made by the judiciary (or administrative agency) on a case by case basis. The statutory exceptions to consent, access and correction, for example, are clearly classified into different public interest categories under the 2021 amendments to provide an even clearer picture of the apportionment of rights and interests for the stakeholders (see Table 1 above).

131 See Administrative Appeal No 54/2014 (Case No 2014A02) where *Eastweek* was referred to in relation to the use of personal data by the complainant: <https://www.pcpd.org.hk/english/enforcement/case_notes/casenotes_2.php?id=2014A02&content_type=3&content_nature=&msg_id2=438> (accessed 1 January 2020). It was also noted that a data collector or user does not include persons who "merely read or collected and aggregated personal information in and from the public domain was *prima facie* not considered as compiling information about another individual, and the provisions of the Ordinance did not come into play".

B. "Personal data", the abuse of access rights and the General Data Protection Regulations

80 The GDPR faces a different problem from the Hong Kong approach to the issue of "personal data" and compliance threshold. Although the effects or results ("impact") doctrine to defining personal data is not value neutral, the scope of personal data has become so wide that, together with the strict and limited statutory exceptions to the protection of personal data, data controllers have run into problems in relation to the "abuse" of certain rights by the data subject, in particular access rights.

81 In Europe, the scope of personal data has expanded over the years, inadvertently leading to broader and stronger rights for data subjects. When this conflicts with other public policy interests, it places the responsibility on judges (or administrative decision makers) to decide on a case by case basis which interest should prevail, which could lead to conflicting decisions. An example of just such a problem (that intermingling personal data as a concept with the measure of statutory obligations can cause) arose in the European Court of Justice ("ECJ").

82 In *YS v Minister voor Immigratie, Integratie en Asiel*[132] and *Minister voor Immigratie, Integratie en Asial v M*[133] (collectively, "*YS and Others*"), data subjects requested access to the "minute" in their immigration files. They were third party nationals making immigration applications for residency in the Netherlands. It was the practice then for applicants to be provided with a summary rather than the full report of the "minute" containing the origin of the personal data and with whom this information was shared, but they wanted access to the full version. The "minute" refers to a draft administrative decision that the case officer assessing applications for residency permit by foreign national draw up that contains the reasons to justify the decision. It served as advice and a recommendation for the final decision-maker, although its reasoning can be, and would likely to be, used by the latter in the final decision.

83 The "minute" contains the following information: "name, telephone and office number of the case officer responsible for preparing the decision; boxes for the initials and names of revisers; data relating to the applicant, such as name, date of birth, nationality, gender, ethnicity, religion and language; details of the procedural history; details of the statements made by the applicant and the documents submitted; the legal provisions which are applicable; and, finally, an assessment of the

132 Judgment of 17 July 2014, C-141/12, ECLI:EU:C:2014:2081.
133 Judgment of 17 July 2014, C-372/12, ECLI:EU:C:2013:838.

foregoing information in the light of the applicable legal provisions. This assessment is referred to as the 'legal analysis'".[134]

84 The main question posed to the ECJ was whether the data reproduced in the minute concerning and relating to the data subject as well as the "legal analysis" constituted personal data. In particular, the "legal analysis" was disputed as personal data between the Member States and the applicants. One can appreciate the concerns of the authorities as the case officer and final decision-maker are implicated. It can also affect their freedom in providing an exchange of views or in their considerations and reasoning on immigration matters; since the applicants consider even abstract legal interpretation in the legal analyses, not just that which contains personal information, as personal data for the purposes of the Directive.[135] That was precisely one of the reasons why the policy was changed from one that provided the full minutes to giving only a summary.[136] The ECJ held that all the other personal information collected except for the "legal analysis" (even if it may contain personal data) constitute personal data.[137] Following from above analysis, the ECJ stated that the right of access can be fulfilled by a summary of the minutes, in which non-personal data is not included or redacted as the case may be.

85 In the subsequent case of *Peter Nowak v Data Protection Commissioner*[138] ("*Peter Nowak*"), the data subject wanted access to a corrected script of an accountancy examination set by the Institute of Chartered Accountants of Ireland ("CAI"), which he sat as a candidate (and failed four times). Although he was given some documents containing his personal data, he was not given a correct script of his examination answer that went on to become the main contention of the dispute, which was whether it was a form of "personal data".

134 Judgment of 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel*, C-141/12 ECLI:EU:C:2014:2081 and Judgment of 17 July 2014, *Minister voor Immigratie, Integratie en Asial v M*, C-372/12, ECLI:EU:C:2013:838, para 14.

135 Judgment of 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel*, C-141/12 ECLI:EU:C:2014:2081 and Judgment of 17 July 2014, *Minister voor Immigratie, Integratie en Asial v M*, C-372/12, ECLI:EU:C:2013:838, para 25.

136 Judgment of 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel*, C-141/12 ECLI:EU:C:2014:2081 and Judgment of 17 July 2014, *Minister voor Immigratie, Integratie en Asial v M*, C-372/12, ECLI:EU:C:2013:838, paras 16 and 42.

137 Judgment of 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel*, C-141/12 ECLI:EU:C:2014:2081 and Judgment of 17 July 2014, *Minister voor Immigratie, Integratie en Asial v M*, C-372/12, ECLI:EU:C:2013:838, para 39. The other questions generally relate to whether, even if they are personal data, the data controller may nevertheless not grant access to the full minutes on any legitimate legal basis.

138 Judgment of 20 December 2017, C-434/16, ECLI:EU:C:2017:994.

86 Under the then Data Protection Directive,[139] "personal data" was defined in Art 2(a) as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". The Irish Data Protection Act of 1988 (as amended in 2003) that transposed the Directive into Ireland, where the dispute arose, defined "personal data" in s 1(1) as "[d]ata relating to a living individual who is or can be identified either from the data or from data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller".[140]

87 The CAI refused his request for access on the basis that it did not constitute "personal data", to which the Data Protection Commissioner of Ireland agreed. In an action to the courts, the data subject's request was likewise rejected on the same ground. In the final appeal to the Supreme Court sent the following questions to the ECJ for a preliminary ruling:[141]

> (1) Is information recorded in/as answers given by a candidate during a professional examination capable of being personal data, within the meaning of Directive 95/46?
>
> (2) If the answer to Question 1 is that all or some of such information may be personal data within the meaning of the Directive, what factors are relevant in determining whether in any given case such script is personal data, and what weight should be given to such factors?

88 On 20 December 2017, the ECJ issued a ruling determining that examination answers of an individual constitute personal data. In its ruling, the ECJ made the following clarifications: First, as long as the data controller has available to it the means to "easily and infallibly" identify the candidate of a script (and that there is no requirement for the identification to be on the hands of one person), it is personal data for

139 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive was repealed and replaced by the GDPR. The GDPR contains a similarly broad definition of "personal data". The *Guidelines on transparency under Regulation 2016/679* (Article 29 Working Party, WP260 rev.01) remains relevant, although it ceased operation on 25 May 2018 and has since been replaced by the European Data Protection Board.

140 Subsequently replaced by the Irish Data Protection Act 2018, to give effect to the GDPR.

141 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, para 26.

the purpose of the Directive or Act.[142] Second, the definition of "personal data" is assigned a wide scope, regardless of the nature of the information (*ie*, sensitive or private) and including "subjective information" like opinions and assessments, provided that they relate to the data subject in question.[143] Third, what relates to a data subject is "by reason of its content, purpose or effect, is linked to a particular person", which is consistent with the definition ascribed to "relating to" a person by the Article 29 Working Party's opinion on the concept of personal data.[144] In relation to the third point, the ECJ stated in relation to the content of the examination answers that is specific to the data subject:[145]

> First, the content of those answers reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment. In the case of a handwritten script, the answers contain, in addition, information as to his handwriting.
>
> Second, the purpose of collecting those answers is to evaluate the candidate's professional abilities and his suitability to practice the profession concerned.
>
> Last, the use of that information, one consequence of that use being the candidate's success or failure at the examination concerned, is liable to have an effect on his or her rights and interests, in that it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought.
>
> It is, moreover, equally true that the written answers submitted by a candidate at a professional examination constitute information that relates to that candidate by reason of its content, purpose or effect, where the examination is, as in this case, an open book examination.

89 Certainly, the content was furnished by Nowak, the purpose was to assess his "knowledge and competences" in the field of accountancy,

142 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paras 30–31. The ECJ noted that the CAI could ascribe the answer script to a candidate, having in their possession "information needed to enable it easily and infallibly to identify [a] candidate through his identification number, placed on the examination script or its cover sheet": Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, para 32.

143 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paras 33–34.

144 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, para 35. See also, Opinion 4/2007 (20 June 2007) (Article 29 Data Protection Working Party, 01248/07/EN), available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> (accessed 7 February 2022).

145 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paras 37–40. In contrast to a representative survey to obtain information independent of the person.

and the impact was felt by him in failing the course and its effect on his career (or lack thereof) in this field.

90 The ECJ also stated in relation to the comments on the examination answers by the examiner that:[146]

> The content of those comments reflects the opinion or the assessment of the examiner of the individual performance of the candidate in the examination, particularly of his or her knowledge and competences in the field concerned. The purpose of those comments is, moreover, precisely to record the evaluation by the examiner of the candidate's performance, and those comments are liable to have effects for the candidate, as stated in paragraph 39 of this judgment.

Hence, these also constituted Nowak's personal data, regardless of the fact that they also included information relating to the examiner. This is also regardless of the problems that can entail from the candidate's rights of access to, and rectification of, his personal data, particularly if it relates to opinions rather than facts.

91 This is a reversal of the position taken in *YS and Others*. The decision in *Peter Nowak* adhered more closely to, and is more aligned with, the Article 29 Working Party's opinion on the concept of personal data.[147] In both cases, the information on the data subject was collected, used and in some cases shared for the purpose of evaluating him or her, which influenced the status of that individual and had an impact on the data subject's rights and interests in the context of the cases.

92 *Peter Nowak* highlights the questionable limits of "personal data" and the extent to which certain rights (in this case, access rights) should be available to the data subject in relation to a category of personal data that can be considered as sensitive in nature and that can lead to

146 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paras 42–45.

147 See n 144 above. According to the Article 29 Working Party's opinion: "[I]n order to consider that the data 'relate' to an individual, a 'content' element OR a 'purpose' element OR a 'result' element should be present. … That 'purpose' element can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual. … A third kind of 'relating' to specific persons arises when a 'result' element is present. Despite the absence of a 'content' or 'purpose' element, data can be considered to 'relate' to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case."

consequences for an institution (public or private) that would impact its processes, exercise of discretion and independence of decision-making.[148]

93 We see that it can become even more complicated when "evaluative data" of an individual, whether for entrance into an educational institution or in relation to a job application or interview, can include the personal data of another person, such as an assessor or examiner or interviewer, who has a "conflicting" interest and right to privacy and confidentiality relating to the determination in question. Overarching that are public policy concerns on the impact that that can have on such administrative decisions.

94 In this respect, the drafters of the original version of the PDPA took the pre-emptive step of statutorily excluding from the access requirements "opinion data kept solely for an evaluative purpose" (which can apply to, for example, personal information relating to admission or employment decisions) and "any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results" from both access and correction rights.[149] The former issue was dealt with succinctly in *HSBC Bank (Singapore) Limited*.[150] In this case, the complainant wanted to exercise his access rights to the respondent bank's internal evaluative report prepared to consider his credit card application, which was unsuccessful. He was given a report with the evaluative portions redacted, but wanted those parts included. The Commissioner decided that the report contained personal data but that it fell within the exception to access under para 1(*a*) of the Fifth Schedule.

VI. Conclusion

95 In conclusion, this article has drawn from the PDPC administrative decisions as well as relevant statutory provisions to show the dynamic nature of the "reasonableness test" as the backbone of the PDPA and the threshold for the obligations contained therein. The test can be supplemented by other tests where relevant, such as the tests of proportionality, necessity and practicability, which are most

148 Another example of such a dilemma relating to access rights to personal data held by a public authority arose in the cases of *Durant v Financial Services Authority* [2003] EWCA Civ 1746 and *Edem v Information Commissioner and another* [2014] EWCA Civ 92 in the UK, where government agencies are not excluded from the data protection obligations of the UK Data Protection Act 2018 (c 12).

149 Paras 1(*a*) and 1(*b*) of both the Fifth and Sixth Schedules of the Personal Data Protection Act 2012. These provisions remain intact after the recent amendments.

150 [2021] SGPDPC 3.

apparent in relation to the purpose limitation and consent obligations. The administrative decisions, PDPC guidelines as well as the increased inclusion of mandatory (and discretionary) factors and considerations particularly in the 2021 statutory amendments provide more guidance in the reasonableness assessment. This mirrors the development of the fair use doctrine and jurisprudence as a statutory exception to copyright infringement.

96 Second, the flexibility of the concept and scope of reasonableness as the statutory standard is demonstrated by how the approach and considerations can adapt to different objectives, situations and categories of personal data, and how it can be contextualised to the different obligations. This is similar to how the fair use doctrine has developed in tandem with developments in technology in the context of copyright protection. As reasonableness can be a basis to obviate the statutory obligations under the PDPA, similar to how the fair use doctrine operates to legitimise use, it should have the force of a genuine exception rather than as a defence, and there should be a legal obligation on the data subject or complainant and the PDPC to *prima facie* examine and consider in good faith the right of the data controller or organisation to the collection, use or disclosure (as the case may be) of the data before bringing a complaint or investigating such a complaint. This obligation should not be an onerous one, but where it is frivolous, vexatious or not made in good faith, there should perhaps be some form of penalty for it, similar to the action for misrepresentation under the US Digital Millennium Copyright Act in a bad faith copyright action (ignoring a fair use assessment or a clearly applicable fair use exception).

97 Last, but not least, the assessment of reasonableness must also be independent of the definition and scope of personal data to avoid confusion and problems when conflicting interests arises, such as in relation to sensitive or confidential information that includes personal data and where there are stronger public policy grounds to justify an exemption of the individual's rights under the Act.
